Template Version Number: 01-2021

U.S. Department of Commerce
National Institute of Standards and Technology (NIST)

Privacy Threshold Analysis
for the
137-01 Emergency Services Office System

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 137-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

a) Whether it is a general support system, major application, or other type of system

The Emergency Services Office System is a major application comprised of the following components: Physical Access Control Systems (Boulder and Gaithersburg), Visitor Registration System including Visitor's Center Application, and Report Exec Enterprise. These components collectively provide the tools necessary to fulfill its mission to deliver emergency and physical security functions for the protection of personnel, property, and activities on NIST facilities.

b) System location

The system components are located at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities within the continental United States.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

- **The Physical Access Control Systems (Boulder and Gaithersburg) are standalone systems on an isolated network that do not interconnect with other NIST systems.**
- **The Visitor Registration System interconnects with the NAIS (one-way transmission only) for processing foreign national visitors so that their information is processed upon arrival. There is also an API integration with Certain Conference Registration (SSP 107-02) to pull NIST-1260 information for foreign conference attendees. All visitors will be checked against the pre-registered data through the Visitor's Center application during check-in.**
- **Report Exec Enterprise does not interconnect with other NIST systems.**

d) The purpose that the system is designed to serve

The components collectively provide the tools necessary to deliver emergency and physical security services for the protection of personnel, property, and activities on NIST facilities.

e) The way the system operates to achieve the purpose

- **The Physical Access Control Systems (Boulder and Gaithersburg) support physical security operations at NIST Boulder and Gaithersburg campus. These systems include digital video camera and closed-circuit television monitoring of the campus and facilities.**
- **The Visitor Registration System is an internally hosted application for pre-registering all visitors to the NIST campus. The Visitor's Center desktop application is used for printing NIST temporary visitor badges. Registered data and images from scanned identification are used to create the badges. If images from the identification are not clear, then a photo is taken of the visitor. This applies to both domestic and foreign national visitors.**
- **Report Exec Enterprise is an incident reporting and records management software to assist the Police Services Group in Boulder and Gaithersburg in writing detailed investigative reports, tracking daily dispatch calls, and recording other law enforcement activities.**

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The type of information includes: identifying numbers, general personal data, work-related data, distinguishing features/biometrics, and system administration/audit data.

g) Identify individuals who have access to information on the system
Only authorized, role-based access exists given the sensitive mission nature.

h) How information in the system is retrieved by the user
Generally, data will be retrieved manually by name, date, date of birth, or location, but searches can also be done on several other fields within the system.

i) How information is transmitted to and from the system

- **Physical Access Control Systems (Boulder and Gaithersburg): Information is captured from the DN-52 form and HR processing, then manually inputted into the system by ESO staff.**
- **Visitor Registration System: Data is entered by NIST employees or sponsor through a web-based interface during pre-registration. When the visitor arrives, their identification is scanned. The pre-registration data and either the photo taken or image captured from the scanned identification are used to print a NIST temporary visitor badge at check-in. This is all done through the Visitor's Center desktop application. Visitor Registration System is also configured to interface with Certain Conference Registration (SSP 107-02) via an API web service to automatically pull NIST-1260 information and then push that data to the NAIS for DOC OSY review and approval.**
- **Report Exec Enterprise: Information is collected by the police officers and/or dispatch operators directly from the data subject and manually entered into the system for investigation and follow up purposes.**

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

This is an existing information system with changes that create new privacy risks. (Complete chart below, continue to answer questions, and complete certification.)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks
Other changes that create new privacy risks:
Data from scanned identification (name, DOB, photo, etc.), which was previously embedded in images, will now be pulled into separate, searchable fields in the Visitor's Center Application. Pictures will also be taken when ID cannot be scanned or are not clear after being scanned.

1b Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes

Activities
Video surveillance **Building entry readers**
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate sensitive personally identifiable information (PII)?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

Yes, the IT system collects, maintains, or disseminates sensitive PII.

The IT system collects, maintains, or disseminates sensitive PII about:
DOC employees
National Institute of Standards and Technology Associates
Contractors working on behalf of DOC
Other Federal Government personnel
Members of the public

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
The use of the social security number is for the Gaithersburg Physical Access Control System to make a positive identification to prevent identification fraud. The individual's social security number will not be disclosed to anyone external to NIST except as required by law.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

Is a PIA Required?	**Yes**

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the 137-01 Emergency Services Office System and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

The criteria implied by the questions above **do not apply** to the 137-01 Emergency Services Office System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Kelsey, Richard Office: 318/A115 Phone: 303-497-5236 Email: Richard.kelsey@nist.gov Signature: RICHARD KELSEY Digitally signed by RICHARD KELSEY Date: 2022.04.14 13:50:06 -04'00' Date signed: ________________	**Chief Information Security Officer** Name: Heiserman, Blair Office: 225/B048 Phone: 301-975-2065 Email: nist-itso@nist.gov Signature: Digitally signed by BLAIR HEISERMAN Date: 2022.04.18 15:35:19 -04'00' Date signed: ________________
Co-Authorizing Official Name: Vanek, Anita Office: 101/A1124 Phone: 301-9753744 Email: anita.vanek@nist.gov Signature: ANITA VANEK Digitally signed by ANITA VANEK Date: 2022.04.08 15:30:41 -04'00' Date signed: ________________	**Authorizing Official** Name: Sastry, Chandan Office: 225/B222 Phone: 301-975-6500 Email: chandan.sastry@nist.gov Signature: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2022.04.08 14:07:01 -04'00' Date signed: ________________
Privacy Act Officer Name: Fletcher, Catherine Office: 101/A523 Phone: 301-975-4054 Email: catherine.fletcher@nist.gov Signature: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2022.04.11 17:11:00 -04'00' Date signed: ________________	**Chief Privacy Officer** Name: Barrett, Claire Office: 225/B226 Phone: 301-975-2852 Email: claire.barrett@nist.gov Signature: CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2022.04.01 10:33:47 -04'00' Date signed: ________________